WHAT IS CLAIMED IS:

1. A system for securing an application for execution on a computer, the system comprising:

a server computer;

a network; and

a client computer operably connected to the server computer via the network;

wherein the client computer receives from the server computer an application;

wherein the client computer executes the application subsequent to receiving the application; and

wherein the client computer includes an interception module for intercepting a request for computer specific information that is made by the application.

2. A method of securing an application for execution on a computer, the method comprising:

modifying the binary of the application such that a request from the application for machine or user information is intercepted transparently to the application; and

providing fake machine or user information.

3. The method of Claim 2, wherein the request for machine depending information is selected from the following: a request for a machine name, a request for an environment variable, a request for setup information, and a request for IP information.

4. A method of securing an application for execution on a computer, the method comprising:

intercepting a request from the application to open a key in a system database;

determining whether the requested key is in the virtual database;

if the key is not in the virtual database, storing fake information in the virtual database; and

if the key is in the virtual database, returning a handle to the virtual key.

5. The method of Claim 4, additionally comprising inserting in an import table a reference to an interception module, wherein the reference is inserted in the import table such that the interception module is invoked in response to loading of the application, and wherein the interception module intercepts the request from the application.

6. A method of securing an application for execution on a computer, the method comprising:

intercepting a request from the application to open a key in a system database;

determining whether the requested key is in a virtual database;

if the key is not in the virtual database, accessing the key in the system database; and

if the key is in the virtual database, returning a handle to the virtual key.

7. A method of securing an application for execution on a computer, the method comprising:

intercepting requests to open a first key in a system database; and

returning a handle that references a second key in a virtual database.

8. A system for securing an application for execution on a computer, the method comprising:

means for intercepting requests to open a key in a system database;

means for opening a virtual key in a virtual database; and

means for returning a handle to the virtual key.

9. A system for securing an application for execution on a computer, the method comprising:

means for intercepting requests to open a first key in a system database; and

means for returning a handle that references a second key in a virtual database.

10. A system for securing an application for execution on a computer, the system comprising:

an interception module for intercepting requests to open a key in a system database, wherein the interception module opens a virtual key in a virtual database, and wherein the interception module returns a handle to the virtual key.

11. A program storage device storing instructions that when executed perform the steps comprising:

intercepting requests to open a key in a system database;

opening a virtual key in a virtual database; and

returning a handle to the virtual key.

12. The program storage device of Claim 11, additionally comprising:

opening a system database key in the system database;

modifying a key value that is associated with the system database key; and

associating in the virtual database the modified key value with the virtual key.